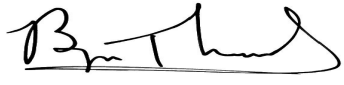


**RICHMOND POLICE DEPARTMENT GENERAL ORDER**

NOTE: This directive is for internal use only, and does not enlarge an employee's civil liability in any way. It should not be constructed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this department, and then only in a non-judicial administrative setting.

Series 3	Number 5	Effective Date 07/09/09	Review Date 2012
Subject ELECTRONIC SYSTEMS AND EQUIPMENT			New Order ☒ Replaces G.O. 3-5 (01/10/05) E.O. 07-14 (09/26/07)
References <i>CALEA 41.3.7a, 41.3.7b, 81.2.10</i> City Administrative Regulations 2.1, 2.2, 2.3, 2.4, 2.5, 6.2 VLEPSC OPR .01.06 <i>General Order 6-14, Digital Mobile Video Recorder System (DMVR)</i>			
 _____ Chief of Police or Designee		07/09/09 _____ Date	

I. PURPOSE

The purpose of this directive is twofold. First, to establish the guidelines for the proper use of the electronic systems and equipment utilized by the Department. Second, to establish the proper use of Internet and Intranet technology using software and hardware provided by the City of Richmond to its employees for the purpose of performing job functions that include communication, information exchange and research.

II. POLICY

- A. Electronic systems and equipment allows the Richmond Police Department enhanced communication abilities for both routine and emergency situations. This enhancement can be communication and notifications during unusual occurrences, hostage/barricade incidents and Department mobilizations, and allows for efficient and effective information relays between the various components of the Department.
- B. It is the policy of the Department that employees use its electronic systems and equipment for business activities of the Richmond Police Department as a means to further the Department's mission by providing services that are efficient, complete, accurate and timely.
- C. The Department reserves the right to monitor any of its electronic systems, including E-mail messages and any other known messages, documents, spreadsheets or files. It is also the policy of the Department that members shall not read messages received by another employee when there is no business reason for doing so, nor shall any member send any electronic message under another employee's name or change any portion of a previously sent electronic message without proper authorization.

- D. The Department's electronic systems and equipment shall not be used to promote discrimination on the basis of race, color, national origin, age, marital status, sex, political affiliation, religion, disability or sexual preference, to promote sexual harassment or to promote personal, political or religious business or beliefs.

III. ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this general order. Failure to comply will result in appropriate corrective action. Responsibility rests with the Division Commander to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated.

IV. DEFINITIONS

- A. ELECTRONIC SYSTEMS – All hardware, software, and tools owned by the City of Richmond available for official use by City employees including but not limited to electronic mail, voice mail, calendaring and systems such as INTERNET, etc.
- B. INTERNET SYSTEM – A global information system of interconnected computers and computer networks used to receive and transmit information and electronic messages.
- C. INTRANET SYSTEM – A local information system used to receive and transmit information and electronic documents among authorized users.
- D. MOBILE DATA COMPUTER (MDC) – The hardware device used by officers in the field to run communications, NCIC/VCIN inquiries, and other software applications. The term MDC shall apply to both the fixed mounted and laptop versions.
- E. ***DIGITAL MOBILE VIDEO RECORDER (DMVR) – Equipment installed in patrol vehicles which is used to record a video/audio account of events.***
- F. ***WIRELESS COMMUNICATION DEVICES – Wireless communication devices shall be defined as cellular telephones, Blackberry units, or any other electronic communication devices and services, to exclude City owned radios which are provided by the city.***

V. PROCEDURE

- A. Electronic Mail (E-mail) Usage:
 - 1. Electronic mail is a Department resource and is provided as a business tool. It shall be used to augment other types of communication already in the workplace such as the telephone, fax machine, voice mail, written memorandum, and the like.
 - 2. E-mail messages shall be treated like paper memos, faxes and the like, with regard to privacy. When a paper memo, fax, or e-mail has left the sender, he/she relinquishes the domain over it.

NOTE: Confidentiality/Privacy – All departmental electronic systems are public record and subject to inspection and disclosure. Employees have no expectation of privacy in their use of electronic mail.

3. Marking a message “private” in the E-mail system does not prevent the Department from having access to an employee’s mailbox nor will it inhibit the viewing of all contents.
4. Any department-wide E-mail to “Police — All Personnel” should be sent out by a Captain/Civilian Manager *or designee* of a Division or above.

NOTE: The only exception for department-wide E-mails is in Administration, with notification to all department personnel by Computer Services personnel regarding automated systems issues.

5. E-mail users shall exercise caution in logging in and out of the electronic system to prevent someone else from utilizing their password to send messages.

NOTE: When in doubt, Department members should not E-mail information.

6. Members desiring to retain hard copies of E-mail messages should utilize the procedures used by the Department for other types of correspondence.
7. Inappropriate Uses:

Personnel will not transmit by any electronic device:

- a) Pornographic images or text (except as needed for investigative or intelligence gathering purposes – and only by personnel previously authorized by the *Executive Director*, Major *or Division Head* of the affected Operation or Service);
- b) Chain letters;
- c) Images or text that are harassing, intimidating, hostile, offensive, retaliatory or otherwise discriminatory based upon race, gender, color, national origin, ethnicity, sexual orientation or disability;
- d) Group messages to “Police – All Personnel”, or any other universal address, unless sent by a Captain or higher or Civilian Division Manager, or designated members of Computer Services);
- e) Solicitations;
- f) Political endorsements or messages; or,
- g) Unethical, illegal, unprofessional, or disruptive activities.

B. Internet and Intranet Systems:

Internet and Intranet systems are provided by the City of Richmond for the purpose of conducting City business. Allowable use includes the following:

- 1) To facilitate performance of job functions;
- 2) To conduct research in accordance with an employee's job duties and functions; and,
- 3) To communicate with other outside organizations as required *for the performance of* job functions.

C. ***Wireless Communication Devices:***

1. Department-Issued Cellular Phones(*including Blackberry units*):

- a. Department-issued ***wireless communication devices*** are primarily for official use only. Members are to use cellular phones sparingly and judiciously *for business purposes*.
- b. Selected individuals may use cellular phones with the expenses paid as per City policy. Authorization will be determined by the Major, ***Executive Director or Division Head*** of the affected Operation/Service, which shall be based on the need for frequent or immediate access to the individual, the impact on efficiency, and/or cost effectiveness.

NOTE: The authorization to obtain additional Blackberry units shall be based on the approval of the Assistant Chief of Police or designee. Supervisors of an employee(s) who has not previously been issued a Blackberry and is currently requesting a Blackberry shall notify Computer Services. The Computer Services unit shall be responsible for forwarding a justification letter to the Assistant Chief of Police requesting authorization approval. Upon approval, Computer Services shall forward the signed justification letter to the City Finance office. The receipt of funding shall complete the process to move forward with purchase and obtaining a Blackberry unit.

NOTE: Per Richmond Administrative Regulation numbers ***2.3 and 6.2***, employees are NOT to use a ***wireless communication device*** while actively driving a city vehicle.

2. Responsibility for Cellular Phones and Pagers:

- a. Each Major, Executive Director ***or Division Head*** shall be responsible for ensuring that the cellular phones and pagers are assigned throughout his/her Operation/Service according to current operational needs and requirements.
- b. Administration shall record and maintain a listing of all Department-issued cellular phone numbers and pager numbers, and to whom they were assigned (except those used in undercover assignments). This listing shall be regarded as confidential. These numbers and assignments shall not be

provided to anyone outside of the Department without proper authorization. However, an individual member may provide his/her issued cellular phone number or pager number to family members and to select others for limited personal use.

- c. It is the responsibility of Department members who are assigned Department-issued equipment to ensure that it is secure at all times, and users of cellular phones are also responsible for ensuring authorized use.

NOTE: Members who lose or damage Department-issued equipment through misuse, negligence, or abuse will be required to reimburse the Department for any replacement or repair costs.

3. Cellular Phone Billing Statements:

- a. Any cellular phone billing statement submitted for reimbursement shall be subject to disclosure in accordance with the Freedom of Information Act. These records shall be forwarded, upon request, to the City Attorney's Office through the Office of **General Counsel**.
- b. Both incoming and outgoing calls are charged to the Department's cellular phone account for its cellular phones.
- c. Whenever possible, the Department member shall use the police radio or a nearby available private or public telephone to communicate. A cellular phone shall only be used for those situations where its use arises out of operational necessity. Cellular phone users shall be required to reimburse the Department for all calls made inappropriately.
- d. If a Department member experiences any technical problems with the operation of his/her cellular phone, the OIC of the affected division/unit shall contact the OIC of the Financial Management Purchasing Unit as soon as possible.

NOTE: Cellular phone calls can be monitored by various types of electronic equipment available to the general public. Cellular phone conversations may also be picked up inadvertently on other communication devices. All police personnel are encouraged to exercise caution when discussing sensitive and confidential information when using a cellular phone.

- e. Long Distance Telephone Calls – Any personal long distance call must be made collect or using a personal calling card.

4. Use of Pagers:

- a. Certain duty assignments require the use of pagers. The Chief of Police, Assistant Chief, **Executive Director**, Majors **and Division Head** designate the assignments. The Department also allows some of its members to carry privately owned pagers. All Department members are prohibited

from using pagers or other electronic devices to contact secondary employment while on duty.

- b. *Any* Department member *issued a pager, cell phone and/or Blackberry* shall be required to wear or keep *the issued equipment* near them at all times to ensure that they remain on-call 24 hours a day. This ensures that the members can be contacted during emergencies even when the member's electricity or telephone services are out of order.
- c. Uniformed members while on duty must wear their pagers on the uniform belt. The pager worn in other places, such as on shirt epaulets, is prohibited. The carrying case for a pager should be non-descriptive or inconspicuous.
- d. If a Department member experiences any technical problems with the operation of his/her pager, *he/she* shall contact *the Computer Services Help Desk for assistance*.

5. Mobile Data Computer (MDC):

a. Training and Security:

- 1. Officers using the MDC must acquire and maintain a minimum of VCIN Class C certification prior to accessing the VCIN queries.
- 2. Information obtained through VCIN/NCIC is for criminal justice use only and may not be disseminated or provided to non-criminal justice personnel, unless otherwise prescribed by law.
- 3. Officers will ensure that no unauthorized person can view the information on the MDC screen at any time.
- 4. All Department vehicles containing a MDC must be secured while they are unattended.
- 5. Officers are reminded that all queries sent over the MDC are recorded and can be retrieved for review.

b. Communication and Usage:

- 1. If available, the MDC should be used for routine communications including car to car messaging, VCIN/NCIC inquiries, and call for service information. By utilizing the MDC, the radio is kept clear for emergency traffic. This does not preclude officers or dispatchers from using the radio during emergencies, for officer safety reasons, or when officers are away from their vehicles.

- 2. Information that is sent via car to car messaging should be limited to short messages that are appropriate in nature. Generally, if inappropriate for the radio, it is also inappropriate for the MDC. The

same standards for radio communication apply to MDC communications. Officers shall refrain from using obscene, indecent or profane language and shall keep all transmissions on a professional level.

NOTE: All vehicles equipped with a MDC shall be used in a manner that is conducive to the safe operation of the motor vehicle.

c. Care and Maintenance:

1. Officers are responsible for the use and care of the MDC in their possession. Officers that damage the MDC through misuse, negligence, or abuse may be required to reimburse the Department for any replacement or repair costs.
2. Officers should not place drinks, food, or other items that may cause damage near or directly on the MDC.
3. Only Computer Services or authorized personnel may add, delete or modify the software on the MDC.

D. Use of Digital Cameras:

1. Officers *may* be issued a digital camera to enhance their ability to perform their job functions. Supervisors shall record the issuance of each digital camera and further document that the officer(s) have been notified in writing of these protocols. The issuance of the departmental digital camera is a job enhancement *tool* and it is neither an entitlement nor a guarantee. Therefore, it is subject to revocation for *at any time*.
2. When officers anticipate using photographs as evidence in a criminal or civil proceeding, the officer shall immediately move those photographs into *his/her* network drive (H:). Each assigned camera will download the officer's images to his or her network (H:) drive. No other copies of the photographs should be made to the network, individual personal computer, or other removable media.
3. At the end of each shift, officers shall download all photographs, excluding those subject to *the 'Communications and Usage' section of this order*, onto their individual files on the officers individual network drive (H:). When downloading individual images, officers will use their file name, report number or camera date as provided. All photographs will remain on this drive unless they are moved per one of the other provisions listed in this Order.
4. Officers shall not browse through photographs taken by other officers that have been moved to the X drive (except for those posted to X:/Daily Briefings) unless directed to do so by their immediate supervisor. Investigating officers requesting photographs to be placed on the X drive will delete that folder immediately after use.

5. All photos taken are the property of the Richmond Police Department.
6. Officers may and are encouraged to practice while on duty with the digital camera on non-work related subjects but may not take, print, download, or distribute any photos that may discredit the Department.
7. There will be no manipulation of the original photographs either by the officer that took the photograph or by any member of this police department. At no time will original evidentiary photographs be altered. Any manipulation to original photographs will be tracked by the department's information systems.
8. No digital photographs classified as evidence will be stored by and/or transmitted to other individuals outside the Richmond Police Department unless specifically authorized in writing by a supervisor.
9. No digital photographs will be posted on the Internet without the express written consent of the Chief of Police or designee.
10. Crime scenes that are customarily photographed by forensics detectives (including but not limited to homicide scenes) shall not be photographed by officers with their digital camera unless directed to do so by either their immediate supervisor or a Forensic Unit supervisor or designee. If photographs are taken prior to the arrival of forensics and or detectives, these photographs are to be turned over to the Forensic Unit.

E. Use of the *Magistrate's* Video *Teleconferencing* Equipment:

The Magistrate's Office's Video *teleconferencing* equipment will be online and utilized by police officers for processing arrests and obtaining warrants. The following protocol shall be followed:

1. The officer will respond to the Warrant *and Information Services Unit* (Information desk) to obtain the criminal history record.
2. If the officer has not already been trained in the use of the video *teleconferencing* equipment, he/she must inform the *Magistrate's office* who will offer assistance.
3. Sally Port location - The officer shall ensure that the sally port gate is secured, and will lock his/her firearm in the gun box prior to removing the prisoner from the transport vehicle and using the video *teleconferencing* equipment.
4. The officer will *properly* fax the CCRE to the magistrate *and ensure its receipt*.
5. The magistrate will receive the fax, which will also serve as an official notification that an officer has an arrestee in the sally port location, police headquarters *or precinct*.

6. The magistrate will then activate the officer's location and either immediately start the probable cause hearing or provide a time frame in which the hearing will start.
7. The suspect's criminal history will be verbally read to the magistrate via video.
8. Once the hearing has occurred and the magistrate is ready to issue a warrant, the officer will be instructed as to what form(s) to place in the printer.
9. The magistrate will then start the printer process from his/her location. Officers are NOT TO TOUCH ANY EQUIPMENT UNLESS AUTHORIZED TO DO SO, *with the exception of* the fax machine.
10. After receiving the warrant(s) and any other paperwork, the officer will proceed to lock-up and relinquish the prisoner to the Richmond Sheriff's Office.
11. The logbook inside the video *teleconferencing room* is for process time record purposes and will be filled out completely at the beginning and end of each arrest.

NOTE: For safety and control reasons, arrestees will be handcuffed behind their backs during the video conferencing process unless there are specific justifications for doing otherwise.

F. ***Emergency Operations Center (EOC):***

1. ***Video teleconferencing equipment in the EOC shall be in use during emergencies as directed by the Chief of Police or designee as an emergency command center.***
2. ***While the location and function of the EOC may involve other operational purposes, i.e. training, roll-call, etc., the use of the video teleconferencing equipment must be authorized by the Chief of Police or designee prior to use.***

G. ***Use of DMVR System:***

Employees shall refer to General Order 6-14, Digital Mobile Video Recorder System (DMVR) for all procedures governing the operation of DMVR equipment.

VI. **ROLES AND ACCOUNTABILITY**

A. ***Police Personnel shall:***

1. ***Exercise caution and adhere to all directives regarding the proper use of electronic and wireless communication systems;***
2. ***Not use a wireless communication device while actively driving a city vehicle;***
3. ***Ensure that assigned equipment is secure at all times and used for authorized purposes;***

4. *Wear or keep issued pagers, cell phones and Blackberries near at all times;*
5. *Be responsible for replacement or repair costs resulting from lost or damaged issued equipment;*
6. *Be responsible for billing statements involving any personal calls on Department-issued cellular phones;*
7. *Notify the OIC of Financial Management when experiencing technical difficulties with cellular phones;*
8. *Notify the Computer Services Help Desk when experiencing technical difficulties with pagers or Blackberry units;*
9. *Acquire and maintain any required certification as directed in this order;*
10. *Not disseminate any information received through Department-issued electronic systems; and,*
11. *Follow specific procedures for the use of video teleconference equipment.*

B. Supervisors shall:

1. *Ensure that a current list of equipment and a record of issuance is maintained;*
2. *Direct officers to photograph crime scene, when applicable; and,*
3. *Ensure that crime scene photographs taken by the officer are submitted to the Forensics Unit.*

C. Forensics Unit personnel shall:

Direct officers in photographing crime scene, when applicable.

D. Warrant and Information Services Unit shall:

Provide criminal history record when requested by officer.

E. Computer Services Unit personnel shall:

1. *Disseminate authorized department-wide E-mail messages;*
2. *Be authorized to modify MDC software;*
3. *Provide Blackberry units with authorized written approval and upon receipt of funding; and,*
4. *Assist authorized Department users with technical difficulties involving pagers or Blackberry units.*

F. *Captain/Civilian Manager of a Division or above shall:*

1. *Be authorized to issue department-wide "All Personnel" E-mails;*
2. *Contact the division's official pager liaison if a department member under his/her command experiences technical pager problems; and,*
3. *Designate an official pager liaison for his/her division.*

G. *Assistant Chief of Police, Major, Executive Director or Division Head of Affected Operation/ Service shall:*

1. *Authorize, when necessary, the use of pornographic images and/or text for investigative or intelligence gathering purposes only;*
2. *Authorize request for additional Blackberry units;*
3. *Authorize expenses paid by the City for cellular phone usage; when applicable;*
4. *Ensure that a record is maintained which lists all communication devices and phone numbers assigned to each; and,*
5. *Authorize reimbursement for Department members' use of private cellular phones to conduct Department business.*

H. *Chief of Police or designee shall:*

1. *Designate assignments for use of department-issued pagers;*
2. *Provide written authorization to post the Department's digital photos on the Internet or Intranet; and,*
3. *Authorize the use of video teleconferencing equipment in the EOC.*